www.biometrics.dod.mil

2011 DoD BIOMETRICS COLLABORATION FORUM

Friendly Biometric Credentials

BIMA BIOMETRICS IDENTITY MANAGEMENT AGENCY

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **JAN 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE **Friendly Biometric Credentials**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Research and Engineering,Biometrics Identity Management Agency (BIMA),Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
presented at the 2011 DoD Biometrics Collaboration Forum held 25-27 Jan.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**27**	

Friendly Biometric Credentials Part I

- Friendly Biometrics Quick Look Team
- “Tower of Babel”
- Simple, Bigger Challenges
- Use Cases
- The Good
- The Bad
- & The Ugly

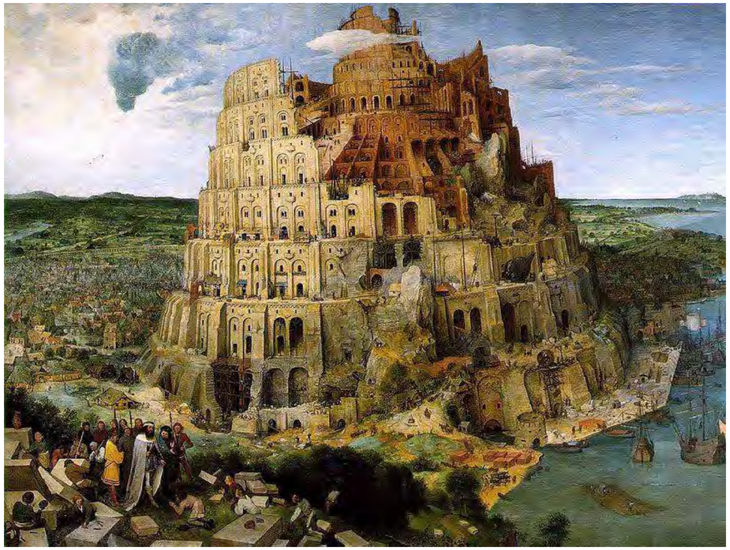
IPMSCG Quick Look Team: Friendly Force Biometrics

- 26 Mar 2010, the IPMSCG established a Quick Look Team (QLT) to identify ways DoD could enhance friendly-force identity management (IdM) capabilities with biometrics.
- BIMA & USD(I) was requested to address the findings
  - Finding 1 – **Physical Access and Biometrics**
    - *Establish TTPs to support biometrically enabled Physical Access Control Systems (PACS)*
  - Finding 2 – **Diverse Modalities and Implementations**
    - *Efficient & effective choices for biometrics solutions*
  - Finding 3 – **Multiple Biometric Repositories**
    - *Establish authoritative sources to "collect once – use often"*
  - Finding 4 – **DoD Enterprise Architecture**
    - *Requirement driven solutions provide efficient IT investments*
- Results briefed to IPMSCG 27Sep 2010
- BIMA is currently staffing / planning Quick Look Transition Plan.

IdM *Tower of Babel*

- IdM issues spans business, warfighter and defense intelligence mission areas. Each community and sub-communities apply different meaning to seemingly common terminology.

- **Objectives:**
  - Agree that we have communications challenges
  - Establish a framework to discuss biometrics role in Identification & Access Control
  - Identify challenges & issues to enable effective, efficient and accurate application of biometrics DoD-wide



"Credential"

Source	Definitions
Office of Management and Budget (OMB) 04-04 E-Authentication Guidance for Federal Agencies	*an **object that is verified when presented to the verifier in an authentication transaction***
Federal Information Processing Standards (FIPS) 201-1, Personal Identity Verification of Federal Employees & Contractors*	***evidence attesting to one's right to credit or authority**; in this standard, **it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual**.*
Committee on National Security Systems Instruction (CNSSI) 4009, Information Assurance Glossary*	***evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more then once**.*
National Institute of Standards and Technology (NIST) 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*	***a credential may be a physical artifact (e.g., a PIV Card) or a data object (e.g., a certificate)**.*
NIST SP 800-63, Electronic Authentication Guideline	[a credential] **binds the token to a name and possibly other attributes** that the [registration authority] has verified.

Within DoD it is safe to assume the recognized Credential is the Common Access Card (CAC) and the associated Private Key Infrastructure (PKI) Certificate.

Authentication Overview

- Authentication factors are generally accepted as:
  - Something one has (e.g., a smart card or a token with Public Key Infrastructure (PKI) certificates)
  - Something your are (e.g., biometric, such as a fingerprint)
  - Something you know (e.g., a PIN or a password)
- Multi-factor authentication requires at least two factors be met
- Multiple factors of a single type only count as one factor
- Strength of factor may vary, affecting overall strength of the authentication process

Basic Authorization Process

Authorization generally involves the following basic process:

1. Claim an identity (e.g., through the presentation of something)
2. Verify the claim (e.g., a separate process to validate the claim is legitimate)
3. Authorize privilege
4. Enable privilege (e.g., open a door, unlock a workstation, etc.)

Note: The following series of use cases attempt to outline the different variations to allow biometrics to enable the authentication process

Biometric Alternatives

- The following slides outline the scope of alternatives that have been discussed where biometrics enables access control

- The objectives are to:
  - Specifically define the scope for which biometrics are discussed to enable access control
  - Establish an agreed upon framework to evaluate the different considerations of each alternative
  - Prioritize use cases and identify actions

Reference

Sequence	Current
1. Claim an identity	PIV
2. Verify the claim	PIN
3. Authorize privilege	Resource
4. Enable privilege	Implementation specific

Discussion

- Status quo
- Governed by HSPD-12/FIPS 201-1
- Biometrics used only confirm the identity of the individual at card issuance was the same one who submitted fingerprints for background investigation.
- Does not leverage “something you are”
- Photograph on card allows for visual inspection by a human

Use Case (1 of 4)

Sequence	Alternative 1
1. Claim an identity	Smart Card
2. Verify the claim	Biometric
3. Authorize privilege	Resource
4. Enable privilege	Implementation specific

Discussion

- FIPS 201-1 – *PIV cards shall implement PIN-based card holder activation to allow privileged operations..*
- NIST-SP 800-63 – *biometrics may be used to prove the "trusted identity" is in possession of the token… use of biometrics to "unlock" conventional authentication tokens and to prevent repudiation of registration is identified in this document*
- FIPS 201-1 implies biometrics can not be used in lieu of a PIN to allow privileged operations …
- 2005-2007, The InterNational Committee for Information Technology Standards (INCITS) chartered an ad hoc group to study role of biometrics in this context and provided recommendations for revision of NIST-SP 800-63 and outlined requirements for future work – what is the status?

Use Case (2 of 4)

Sequence	Alternative 2
1. Claim an identity	PIV
2. Verify the claim	Biometric + PIN
3. Authorize privilege	Resource
4. Enable privilege	Implementation specific

Discussion

- Would be in addition to what FIPS 201-1 states – *PIV cards shall implement PIN-based card holder activation to allow privileged operations.*
- Three factor authentication
- NIST-SP 800-63 – *biometrics may be used to prove the "trusted identity" is in possession of the token… use of biometrics to "unlock" conventional authentication tokens and to prevent repudiation of registration is identified in this document*
- 2005-2007, the InterNational Committee for Information Technology Standards (INCITS) chartered an ad hoc group to study role of biometrics in this context and provided recommendations for revision of NIST-SP 800-63 and outlined requirements for future work – what is the status?

Use Case (3 of 4)

Sequence	Alternative 3
1. Claim an identity	Smart Card
2. Verify the claim	Biometric
3. Authorize privilege	Resource
4. Enable privilege	Implementation specific

Discussion

- Not used in conjunction with PKI
- Requires additional S&T in support, in advance of a future AoA
- Would require community acceptance, policy changes, etc.

Use Case (4 of 4)

Sequence	Alternative 4
1. Claim an identity	Biometric
2. Verify the claim	Comparison against enrolled biometric + PIN
3. Authorize privilege	Resource
4. Enable privilege	Implementation specific

Discussion

- Technically feasible
- Details also captured in INCITS study
- Multi-factor authentication; could be enhanced with multi-modal biometrics
- Limited use cases; should only fill in where HSPD-12/FIPS 201 is not practical
- Fails to easily enable visual authentication of role
- Federal & DoD driven policies define a standard credential for Federal/DoD Employees & Contractors.
- Potential as a Non-DoD Credential, but as a efficiency & effectiveness enabling capability "deep" within a secure area, i.e., w/in a perimeter, w/in a secure facility, w/in a secure room.
- What is the Capability Driver for this solution, i.e., DoD has an existing program of record.
- Technology Maturity?

Use Cases (Consolidated)

Sequence	Reference	Alt. 1	Alt. 2	Alt. 3	Alt. 4
1. Claim an identity	PIV	Smart Card	PIV	Smart Card	Biometric
2. Verify the claim	PIN	Biometric	Biometric + PIN	Biometric	Compare against enrolled biometric
3. Authorize privilege	Resource				
4. Enable privilege	Implementation Specific				

Clarification

Sequence	Other Use Case
1. Claim an identity	Biometric
2. Verify the claim	Comparison against enrolled biometric
3. Authorize privilege	Biometric?
4. Enable privilege	Implementation specific

Discussion

- Single-factor authentication; could be enhanced with multi-modal biometrics
- Limited use cases
- HSPD-12 specifies a federal identification standard; FIPS 201-1 has specified this identification standard as the PIV; DoD has interpreted this as the Common Access Card & embedded PKI Certificate.
- Biometrics alone fails to easily enable visual authentication of role.
- Federal & DoD driven policies define a standard credential for Federal/DoD Employees & Contractors.
- Potential as a Non-DoD Credential, but as a efficiency & effectiveness enabling capability “deep” within a secure area, i.e., w/in a perimeter, w/in a secure facility, w/in a secure room.

Simple, Bigger Challenges (1 of 4)

- There are competing perspectives on the role and application of biometrics
- The formal debate is difficult w/out establishing an agreed upon knowledge foundation of biometric technology in the context of DoD Missions

Simple, Bigger Challenges (2 of 4)

- Biometrics represent a class of technologies distinguished by modalities, e.g., fingerprint, iris, facial, palm, voice, etc.
  - Each modality represents a distinct technology within itself
  - Each modality has different performance characteristics
  - Each modality represents different maturities as respective technologies and acceptance in industry and federal space

- **Challenge**: *Is there accepted DoD **standard criteria** that can be applied against biometric modalities to warrant confidence for respective applications? Who are the Modality SMEs in the community?*

Simple, Bigger Challenges (3 of 4)

- Biometrics is predominantly a commercial based technology, often proprietary in application.
  - Vendors?
  - Industry Evaluation?
  - Product Evaluation?

- **Challenge**: *Biometrics value proposition within DoD is to protect privacy, enable physical and logical security, and drive efficiencies- is it warranted to have vendor/industry/technology certifications & policies for biometric solutions / systems?*

Simple, Bigger Challenges (4 of 4)

- Biometrics technologies are applied w/in a biometrics-enabled system to achieve the desired capability objectives.

- **Challenge**: *Can the DoD community of interest do more to distinguish between biometrics technologies and biometrics-enabled systems?*

Biometrics – The Good, The Bad, & The Ugly

- **The Good** – perceived value of biometrics and biometrics-enabled solutions
- **The Bad** – perceived shortcomings of biometrics and biometrics-enabled solutions

The Good

Assertion/Motivation	Justification	Status
A primary motivation for using biometrics is to easily and repeatedly recognize and individual so as to enable an automated action based on that recognition (1)		
Motivations for wanting to automatically recognized individuals can vary a great deal, including (1): • reducing error rates and improving accuracy • reducing fraud and opportunities for circumvention • reducing costs • improving scalability and practicality • increasing physical safety • improving convenience	Almost all benefit and entitlement programs that have utilized biometrics have done so to reduce costs and fraud rates (with the added benefit of possibly improving convenience as well).	
Biometric technology can link a "person" to his or her claims of recognition and authorization within a particular application. (1)		
Numerous applications employ biometrics for one or more reasons (1): • Border control and criminal justice (such as prisoner handling and process) • Regulatory compliance applications (such as monitoring who has access to certain records or other types of audits) • Determining who should be entitled to physical or logical access to resources • Benefits and entitlement management		
Biometrics cannot readily be shared and offer the prospect of closely linking recognition to a given individual (1)		
Biometrics is appropriate for use as either an Identifier or as an Authenticator • as an Identifier, a Biometric may be authenticated with a PIN or Password • as an Authenticator, a Biometric may authenticate User ID, Smart Card, or Token (2)		
Using multiple Biometrics in conjunction as a single factor can strengthen credentials and greatly increase the difficulty in spoofing (2)		

Sources: (1) National Research Council of the National Academies Study, "Biometric Recognition Challenges and Opportunities", 24 Sep 2010, (2) Raytheon presentation: Biometric Impact on Cyber Security

The Bad

Item/Issue	Potential Mitigation(s)	Status
Biometric recognition systems are complex and need to be addressed as such	System-level considerations are critical to the success of biometric systems. Analyses of biometric systems' performance effectiveness, trustworthiness, and suitability should take a broad systems perspective.	
Biometric recognition is inherently probabilistic hence inherently fallible. The chance of error can be made small but not eliminated.	Must be tempered by an awareness of the uncertainty associated with that recognition. System designers and operators should anticipate and plan for the occurrence of errors, even if errors are expected to be infrequent.	
The scientific basis of biometrics—from understanding the distributions of biometric traits within a given population to how humans interact with biometric systems—needs strengthening, particularly as biometric technologies and systems are deployed in systems of national importance.	Fund additional S&T efforts to examine a range of underlying facets of the technologies and the systems in which they are deployed (e.g., sensors, data management, human factors, and testing)	
The field of biometrics would benefit from more rigorous and comprehensive approaches to systems development, evaluation, and interpretation. Presumptions and burdens of proof arising from biometric recognition should be based on solid, peer-reviewed studies of the performance of biometric recognition mechanisms.	Solid, peer-reviewed studies of the performance of biometric recognition mechanisms? Best practices for deployment and use?	
Biometric systems should be designed and evaluated relative to their specific intended purposes and contexts rather than generically. Their effectiveness depends as much on the social context as it does on the underlying technology, operational environment, systems engineering, and testing regimes.	Efforts to determine best practices for T&E of existing and new biometric systems should be sustained and expanded. Careful consideration should be given to making the testing process open, allowing assessment of results and quality measures by outside parties when appropriate. The evaluation of a system's effectiveness needs to take into account the purpose for which the system was developed and how well field conditions were matched.	

Source: National Research Council of the National Academies Study, "Biometric Recognition Challenges and Opportunities", 24 Sep 2010

BACK UP

Finding 1 – Physical Access and Biometrics

- Majority of the 28 biometrics systems identified are used for physical access. When biometrics are employed :
  - Guidance for local enrollments to PACs are incomplete
  - No consistent incorporation of authoritative source

- **Recommendation**
  - Define the minimum criteria for local enrollments across the DoD
  - Ensure local enrollments are tied to authoritative identity sources
    - Local policy determines if biometrics are used

- **Next Steps**
  - **Lead - USD(I)** Coordinate with BIMA
    - Establish standardized enrollment TTPs for the leading modalities (Fingerprint, Iris)

Establish TTPs to support biometrically enabled PACs

Finding 2 – Diverse Modalities and Implementations

- The survey demonstrated diversity of biometric modalities and implementations
  - No standard modality (8 modalities identified)
  - No common implementation of modalities
    - Technical solution
    - Procedures (TTPs)
- **Recommendation**
  - Identify the top modality(s) to effectively focus resources
  - Promote best practices to leverage the top modality(s) identified
- **Next Steps**
  - **Lead - BIMA**
  - Develop the Biometrics Business Functions Framework (BBFF) for planning, evaluating, and implementing biometric solutions appropriate to requirement/need

Efficient & Effective Choices for Biometric Solutions

Finding 3 – Multiple Biometric Repositories

- The survey illustrated that the application of biometrics in DoD is resulting in the collection and existence of a variety of local biometric repositories/sources:
  - Multiple instances of same/similar biometric modality being collected across DoD
  - Multiple biometric local sources exist with no strategy to store once and use often across DoD

- **Recommendation**
  - Define the issues, challenges and DoD's requirement for authoritative biometric sources that can be utilized across all mission areas

- **Next Steps**
  - **Lead - BIMA -** facilitated cross -functional review with USD(P&R) , USD(I)/DIAC, and DoD CIO
    - Create a strategy for authoritative sources
    - Create a strategy for biometric store once and use often across the DoD

Establish authoritative sources for "Collect once – use often"

Finding 4 – DoD Enterprise Architecture

- Analysis of the survey raises these questions :
  - What is the enterprise architecture governing friendly force biometrics?
    - BIMA has an enterprise architecture that defines biometric capabilities and services
    - The Business Enterprise Architecture (BEA) does not elaborate business needs for friendly force biometrics
  - Friendly force biometric requirements and capabilities are not connected
- **Recommendation**
  - Engage, develop and establish friendly force biometric requirements
  - Incorporate requirements in the BEA
- **Next steps**
  - **Lead – BIMA**
  - Craft Business Improvement Plan to impact the BEA 2012 release in conjunction with the IPMWG strategic acitivites

Requirement driven solutions provide efficient IT investments